TRANSMITTAL OF APPEAL BRIEF (Large Entity)	Docket No. DE-000071

In Re Application Of: **Markus BAUMEISTER et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/841,965	25 April 2001	Samson B. LEMMA	20987	2132	6068

Invention: **METHOD OF DYNAMIC DETERMINATION OF ACCESS RIGHTS**

COMMISSIONER FOR PATENTS:

Transmitted herewith in triplicate is the Appeal Brief in this application, with respect to the Notice of Appeal filed on **19 July 2005**

The fee for filing this Appeal Brief is: **$500.00**

☐ A check in the amount of the fee is enclosed.

☒ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **50-0238**

☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Signature

Dated: **17 August 2005**

Kenneth D. Springer
Reg. No. 39,843
Volentine Francos & Whitt, P.L.L.C.
One Freedom Square
11951 Freedom Drive, Suite 1260
Reston, VA 20190
Tel. No. 571-283-0720

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

_____.
(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

cc:

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	09/841,965
Applicant(s)	:	Markus BAUMEISTER et al.
Filed	:	25 April 2001
TC/A.U.	:	2132
Examiner	:	Samson B. LEMMA
Atty. Docket	:	DE-000071

Title: METHOD OF DYNAMIC DETERMINATION OF ACCESS RIGHTS

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Window, Mail Stop **Appeal Brief - Patents**
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

In response to the FINAL Office Action dated 19 April 2005 and the subsequent Advisory Action dated 8 June 2005, finally rejecting pending claims 1 and 3-7, and in support of the Notice of Appeal filed on 19 July 2005, Applicants hereby submit this Appeal Brief.

Real Parties in Interest

Koninklijle Philips Electronics N.V. owns all of the rights in the above-identified U.S. patent application by virtual of an assignment recorded at Reel 012198, Frame 0136.

Related Appeals and Interferences

There are no other appeals or interferences related to this application or to any related application, nor will the disposition of this case affect, or be affected by, any other application directly or indirectly.

Status of Claims

Claims 1 and 3-7 are all pending and all stand rejected. Claim 2 is canceled. Accordingly, the claims on Appeal are claims 1 and 3-7.

Status of Amendments

There are no pending amendments with respect to this application.

Summary of Claimed Subject Matter

The present invention is directed to a network which dynamically determines whether a user has access rights for an access controlled object.

Accordingly, as broadly recited in claim 1, the invention comprises a network (FIG. 1; page 2, line 32), including: terminals (1) (page 2, line 32); a software system (FIG. 2) (page 3, lines 6-9) distributed over all the terminals (1) (page 1, lines 1-2, 9-11; page 2, line 5); and at least one access controlled object (14) (FIG. 13; page 4, line 4), wherein the software system (FIG. 3) includes at least a filter (9) (page 3, lines 10-11) which evaluates access rights of a user for the access controlled object (14) based on data which are not available until the time of access (page 3, lines 17-20), the filter further evaluating additional data occurring while the user has access to the access control object (14) (page 4, lines 14-16), monitoring a change in the access rights (page 3, lines 23-24), and triggering withdrawal of the access rights to the access controlled object (14) (page 3, lines 24-26).

As broadly recited in claim 3, the invention further features a resource manager (12) which withdraws the access rights (page 3, lines 29-31).

As broadly recited in claim 4, the invention further features an access right

manager (8) (page 3, lines 10-11) which, together with the filter (9), is instructed by the resource manager (12) to check the access rights (page 4, lines 2-8, 12-16).

As broadly recited in claim 5, the invention comprises a network (FIG. 1; page 2, line 32), including: a plurality of terminals (1) (page 2, line 32); a plurality of access control objects (14) (FIG. 13; page 4, line 4); and a software system (FIG. 2) (page 3, lines 6-9) distributed among the terminals (1) (page 1, lines 1-2, 9-11; page 2, line 5), the software system further comprising, an access rights manager (8) (page 3, lines 10-11) and a filter (9) (page 3, lines 10-11) which evaluates access rights of users to access the access control objects (14) (page 3, lines 11-12), wherein the access rights manager (8) has a data structure in the form of a tree (15) (FIG. 6; page 4, lines 3-5) for arranging the access controlled objects (14) and wherein the tree (15) (FIG. 6) includes a plurality of nodes (35-44) which each contain a list of permitted users or user groups respectively (page 5, lines 12-13, 18-28)), of an access controlled object (14) and for each user or user group respectively, include a list of methods of use (page 5, lines 32-34).

As broadly recited in claim 6, the invention further features the filter (9) being adapted to further evaluate additional data occurring while a user has access to an access control object (14) (page 4, lines 14-16), monitoring a change in the access rights (page 3, lines 23-24), and triggering withdrawal of the access rights to the access controlled object (14) (page 3, lines 24-26).

Accordingly, as broadly recited in claim 7, the invention comprises a network (FIG. 1; page 2, line 32) including: a plurality of terminals (1) connected by a bus (2) (FIG. 1; page 2, lines 32-33); a plurality of access control objects (14) (FIG. 13; page 4, line 4); and a software system (FIG. 2) (page 3, lines 6-9) adapted to reserve use of a first one the access control objects (14) by a user via one of the terminals (1) (FIG. 4; page 4, lines 17-30), wherein the software system further comprises a filter (9) adapted to continuously monitor dynamic data affecting access rights to the first control object (14) (page 4, lines 14-16) and, in response to the dynamic data, to generate a message (29) indicating withdrawal of the access rights of the user to the first access control object (14) (FIG. 5; page 4, lines 32-33), the software system being adapted to release (30) the reservation of the first access control object (14) in

response to the message from the filter (9) (page 5, lines 5-11).

Grounds of Rejection to be Reviewed on Appeal

The Grounds of Rejection to be reviewed on Appeal are:

1) The rejections of claims 1, 3, 4 and 7 under 35 U.S.C. § 102 over Peterka International Publication WO99/66714 ("Peterka"); and

2) The rejections of claims 5 and 6 under 35 U.S.C. § 103 over Peterka in view of Brown et al. U.S. Patent 5,941,947 ("Brown").

Arguments

Claims 1, 3, 4 and 7 Are All Patentable Over Peterka

The Office Action dated 8 June 2005 rejected claims 1, 3, 4 and 7 under 35 U.S.C. § 102 over Peterka.

Applicants respectfully traverse those rejections and submit that claims 1 , 3, 4, and 7 are all patentable over Peterka for at least the following reasons.

Claim 1

Among other things, in the network of claim 1 a filter further evaluates additional data occurring while the user has access to the access control object, monitors a change in access rights for the access control object, and triggers withdrawal of the access rights to the access controlled object.

Applicants respectfully submit that Peterka disclose no such features.

The Examiner states that Peterka supposedly discloses the following features in the following text: "***the filter further evaluates additional data occurring while the user has access to the access control object***" (citing page 20, line 28 – page 21; page 31, lines 19-28); "***the filter monitors a change in the access rights***" (citing page 21, lines 11-20 and page 21, line 21 – page 22, line 14; and page 31, lines 19-28); and "***the filter triggers withdrawal of the access rights to the access controlled object***" (citing page 22, lines 22-33 and FIG. 3, ref 370).

Applicants respectfully disagree, and respectfully submit that none of the

portions of text cited above discloses any of these features.

I. The filter further evaluates additional data occurring while the user has access to the access control object

The filter of claim 1 evaluates additional data occurring **while the user has access to the access control object**. For one example, as disclosed in Applicants specification at page 3, lines 24-26, while a user (e.g., a child) is accessing a television program, the filter may continue to evaluate the total time that the user has accessed the television set.

Applicants respectfully submit that Peterka does not disclose any such feature. In particular, Peterka does not disclose such a feature in the cited text at page 20, line 28 – page 21, or page 31, lines 19-28. The cited text at page 20, line 28 – page 21 pertains to determining whether a condition is satisfied **before** the user has access to the access control object. In that regard, reference is made to FIG. 3, and steps 380 and 390 which clearly show that the condition is checked before access is allowed, and to the claims, e.g., claim 1 steps (e)(i) and (e)(ii). That is, in the cited text of Peterka, although the user has the required **permission**, the user does not yet have **access** to the access control object. The Office Action does not cite anything in Peterka that indicates that a user already has **access** to the access control object when the check is made as discussed at page 20, line 28 – page 21. Similarly, the cited text at page 31, lines 19-28 states that when a user attempts to access another access control object, the access may be denied. The text does not state or imply that any filter further evaluates additional data occurring **while the user has already gained access to the channel**.

Accordingly, Applicants respectfully submit that Peterka does not disclose that any filter further evaluates additional data occurring while the user has access to the access control object.

II. The filter monitors a change in the access rights

The filter of claim 1 monitors a change in the access rights while the user has access to the access control object. For one example, as disclosed in Applicants specification at page 3, lines 24-26, while a user (e.g., a child) is

accessing a television program, the total time that the user has accessed the television set may exceed the maximum allowable time such that the access rights are changed.

Applicants respectfully submit that Peterka does not disclose any such feature. In particular, Peterka does not disclose such features in the cited text at page 21, lines 11-20 or page 21, line 21 – page 22, line 14. The cited text at page 21, lines 11-20 discusses changes in the current environment **before** the user has access to the access control object. That is, in the cited text of Peterka, although the user has the required **permission**, the user does not yet have **access** to the access control object. The Office Action does not cite anything in Peterka that indicates that a user already has access to the access control object when the current environment is evaluated as discussed at page 21, lines 11-20. Meanwhile, the cited text at page 21, line 21 – page 22, line 14 discusses conditions generally, but does not indicate that any filter monitors a change in the access rights while the user has access to an access control object. Finally, the cited text at page 31, lines 19-28 states that when a user attempts to access another channel (access control object), the access may be denied. The text does not state or imply that any filter monitors a change in the access rights occurring while the user has already gained access to the channel.

Accordingly, Applicants respectfully submit that Peterka does not disclose that any filter monitors a change in the access rights while the user has access to the access control object.

III. The filter triggers withdrawal of the access rights to the access controlled object

The filter of claim 1 triggers **withdrawal of the access rights** to an access control object to which a user already has access. For one example, as disclosed in Applicants specification at page 3, lines 24-26, while a user (e.g., a child) is accessing a television program, and then the maximum allowable time for using the television set elapses, the filter causes the access rights to be withdrawn. Applicants respectfully submit that Peterka does not disclose any such feature. In particular, Peterka does not disclose such features in the cited text at page 22, lines

22-23. Indeed, in contrast, the cited text at page 22, lines 22-23 indicates that a condition is checked **before** a requested receiver function is allowed. Thus, at page 22 lines 29-31 the text states that if the condition is not satisfied, the call fails and the **original request to invoke the receiver function is denied**. Nowhere does the cited text suggest that if the original request if granted, a filter may later trigger withdrawal of the access rights. Meanwhile, the Office Action cites FIG. 3, element 370 as supposedly disclosing a step of triggering withdrawal of the access rights to an access control object to which a user already has access. However, inspection of FIG. 3 of Peterka shows that the user does not yet have access to the access control object at step 370, and that access is only granted at step 390. Therefore, it is not possible to trigger a withdrawal in step 370 of rights that are not even granted until step 390!

Indeed, Applicants respectfully submit that nowhere in FIG. 3 is there any disclosure or mention of evaluating additional data occurring while the user has access to an access control object, monitoring a change in the access rights, and triggering withdrawal of the access rights to the access controlled object. Inspection of FIG. 3 shows the once a function call is made (330), and the condition is met (380), the function is allowed (390) and that is the end of the process. There is nothing in FIG. 3 which discloses that access rights are ever dynamically withdrawn during an access which has already been granted. Meanwhile, Peterka specifically discloses that his invention "evaluates the current conditions . . . **before** granting permission," (page 33, lines 5-9) but does not state that conditions are further evaluated while access is in progress.

In the Advisory Action, the Examiner states the following:

> "While the children (sic) has already access to the control object/program the system will monitor the time and the current viewer whether or not the current viewer is a child or an adult. This means the system will inherntly (sic) checks (sic) the identity of the viewer by prompting the user to enter their appropriate personal identification

number as explained on page 26, lines 26-31. Just before the predetermined time that is set for the viewer is expired the system will inherently verify the identity of the viewer by checking their Pin and if the viewer is an adult the user will be allowed to continue accessing the control objects. Imagine the scenario where an adult tries to continue accessing the control object or program which the child is already given access to the control objects or TV program but already given time restriction, The (sic) adult just put his/her Pin and be able to continue accessing the control object."

Unfortunately, this is not disclosed anywhere at all in Peterka! Here is the entire cited text at page 26, lines 26-31 of Peterka:

> Permissions can be also associated with a user, such as in the case above, where some users can do e-commerce, IPPV, etc. and some can't. Applications can therefore be run on behalf of certain users. The current viewer can be determined by having the viewer enter a personal identification number (PIN)

Clearly, there is nothing in the cited text regarding children. The cited text also does not disclose any of the following things mentioned by the Examiner: (1) if a child has already access to a control object the system will monitor the time and the current viewer whether or not the current viewer is a child or an adult; (2) just before the predetermined time that is set for the viewer is expired the system will inherently verify the identity of the viewer by checking their Pin and if the viewer is an adult the user will be allowed to continue accessing the control objects (3) a scenario where an adult tries to continue accessing the control object or program which the child is already given access to the control objects or TV program but already given time restriction; or (4) an adult just inputs his/her Pin and will be enabled to continue accessing the control object.

Indeed, Applicants see no mention of these things anywhere in Peterka. This "imaginary" scenario appears to be wholly concocted out of the Examiner's imagination after reviewing Applicants' specification and claims – because it does not appear to be disclosed or remotely suggested by Peterka.

Furthermore, the Examiner states that just "before the predetermined time that is set for the viewer is expired the system will inherently verify the identity of the viewer by checking their Pin." Applicants respectfully traverse this statement and submit that no such feature is inherent in Peterka.

M.P.E.P. § 2112 provides that:

> EXAMINER MUST PROVIDE RATIONALE OR EVIDENCE TENDING TO SHOW INHERENCY The fact that a certain result or characteristic may occur or be present in the prior art is not sufficient to establish the inherency of that result or characteristic. In re Rijckaert, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993) (reversed rejection because inherency was based on what would result due to optimization of conditions, not what was necessarily present in the prior art); In re Oelrich, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is **necessarily** present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.' " In re Robertson, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999). "In relying upon the theory of inherency, the examiner **must** provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic **necessarily** flows from the teachings of the applied prior art." Ex parte Levy, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)

(emphasis added).

Applicants respectfully submit that the Examiner has failed to meet this burden.

Finally, in the Advisory Action, the Examiner also cites page 31, lines 19-28 as supposedly disclosing a feature of monitoring a change in access rights for an access control object. However, the cited text at page 31, lines 19-28 pertains to a an attempt by a user to access a new access control object, not a change in access rights for an access control object which a user already is accessing.

Therefore, Applicants respectfully submit that Peterka does not disclose that any filter triggers withdrawal of access rights to an access control object to which a user already has access.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 1 is patentable over Peterka.

Claims 3-4

Claims 3-4 depend from claim 1 and are deemed patentable for at least the reasons set forth above with respect to claim 1.

Claim 7

Among other things, the network of claim 7 includes: (A) a plurality of terminals connected by a bus; and (B) a software system adapted to reserve use of a first one of the access control objects by a user via one of the terminals, wherein the software system further comprises a filter adapted to continuously monitor dynamic data affecting access rights to the first control object and, in response to the dynamic data, to generate a message indicating withdrawal of the access rights of the user to the first access control object, the software system being adapted to release the reservation of the first access control object in response to the message from the filter.

Applicants respectfully submit that Peterka does not disclose any network including such features.

The Examiner states that he "considers claim 7 to have similar limitation (sic) to claim 1."

Applicants respectfully submit that, contrary to well-established Patent Office guidelines, the Examiner has not specifically addressed all the features of claim 7. Specifically, the Examiner does not cite anything in Peterka that supposedly discloses: (1) terminals connected by a bus; (2) reserving use of an access control object via one of the terminals; (3) generating a message indicating withdrawal of the access rights of the user to the first access control object; or (4) releasing a reservation of the first access control object in response to the message from the filter.

Indeed, the Examiner makes no mention of any bus, reservation, or messages at all!

Respectfully, the burden in rejecting claims over the prior art lies with the Patent Office. Such a burden cannot be met where the Examiner fails to address numerous specifically-recited features of Applicants' claims.

Applicants respectfully submit that Peterka does not disclose any of the features mentioned above.

For example, the Examiner states that he interprets the recited "terminal" to read on Peterka's television receiver. Yet it is fairly clear that Peterka does not disclose any bus connecting a plurality of television receivers. So it is impossible for Peterka to disclose the network of claim 7 that includes a plurality of terminals connected by a bus.

Similarly, Applicants respectfully submit that Peterka does not disclose reserving use of an access control object via one of the terminals; generating a message indicating withdrawal of the access rights of the user to the first access control object; or releasing a reservation of the first access control object in response to the message from the filter.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 7 is patentable over the cited prior art.

Claims 5 and 6 Are All Patentable Over Peterka in View of Brown

Claim 5

Applicants respectfully submit that claim 5 is patentable over Peterka in view of Brown et al. U.S. Patent 5,941,947 ("Brown") for at least the following reasons.

Among other things, in the network of claim 5 an access rights manager has a data structure in the form of a tree for arranging the access controlled objects, wherein the tree includes a plurality of nodes which each contain a list of permitted users or user groups respectively, of an access controlled object and for each user or user group respectively, include a list of methods of use.

Applicants respectfully submit that neither Peterka nor Brown nor any possible combination thereof includes such features.

The Examiner cites Brown col. 2, lines 38-46 as supposedly disclosing such features.

Applicants respectfully disagree.

The cited text in Brown merely discloses that a directory service maintains a directory of content objects as nodes in a tree-like structure. However, the cited text makes no mention of each node containing a list of permitted users or user groups, respectively, of the access controlled object and for each user or user group respectively, including a list of methods of use. Indeed, Applicants see no such disclosure anywhere in Brown. Instead, it appears that Brown uses an access control matrix and access rights database (152) which is **organized by users, not by objects**, and which is organized on a user-by-user (or user-group-by-user-group) basis to list for each user (or user group) the content nodes and access operations available to the **user** (see, e.g., col. 16, lines 39-45 and FIG. 6).

Therefore, Applicants respectfully submit that no combination of Peterka and Brown would ever produce the network of claim 5.

The Examiner fails to explain how one could possibly modify Peterka to include Brown's access control matrix and access rights database which is a **tree for arranging users**, wherein the tree includes a plurality of nodes which each **contain a list of the content and access operations available to the user**, and in the

resulting combination come up with a network that includes an access right manager that has a data structure in the form of a **tree for arranging access controlled objects**, wherein the tree includes a plurality of nodes which each **contain a list of permitted users or user groups respectively**, of the access controlled object **and for each user or user group respectively, include a list of methods of use**, as in claim 5.

Indeed, the Examiner does not even mention the recited list of methods!

So it is impossible that any possible combination of Peterka and Brown could ever produce the network of claim 5

Accordingly, for at least these reasons, Applicants respectfully submit that claim 5 is patentable over Peterka and Brown.

Claim 6

Claim 6 depends from claim 5 and is deemed patentable for at least the reasons set forth above with respect to claim 5, and for the following additional reasons.

Among other things, in the network of claim 6, the filter further evaluates additional data occurring while the user has access to the access control object, monitors a change in the access rights, and triggers withdrawal of the access rights to the access controlled object.

As explained above with respect to claim 1, Applicants respectfully submit that Peterka discloses no such features.

Accordingly, for at least these additional reasons, Applicants respectfully submit that claim 6 is patentable over the cited prior art.

CONCLUSION

For all of the foregoing reasons, Applicants respectfully submits that claims 1 and 3-7 are all patentable over the cited prior art. Therefore, Applicants respectfully request that claims 1 and 3-7 be allowed and the application be passed to issue.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future filings to charge payment or credit any overpayment to Deposit Account No.

50-0238 for any additional fees required under 37 C.F.R. § 1.16, 37 C.F.R. § 1.17, or 37 C.F.R. § 41.20, particularly extension of time fees.

Respectfully submitted,

VOLENTINE FRANCOS & WHITT, P.L.L.C.

Date: 17 August 2005

By: _____
Kenneth D. Springer
Registration No. 39,843

VOLENTINE FRANCOS & WHITT, P.L.L.C.
One Freedom Square
11951 Freedom Drive, Suite 1260
Reston, Virginia 20190
Telephone No.: (571) 283-0724
Facsimile No.: (571) 283-0740

APPENDIX – CLAIMS ON APPEAL

1. A network, comprising:

terminals;

a software system distributed over all the terminals; and

at least one access controlled object,

wherein the software system includes at least a filter which evaluates access rights of a user for the access controlled object based on data which are not available until the time of access, the filter further evaluating additional data occurring while the user has access to the access control object, monitoring a change in the access rights, and triggering withdrawal of the access rights to the access controlled object.

3. The network of claim 1, wherein in the software system further comprises a resource manager which withdraws the access rights.

4. The network of claim 3, wherein the software system includes an access right manager which, together with the filter, is instructed by the resource manager to check the access rights.

5. A network, comprising:

a plurality of terminals;

a plurality of access control objects; and

a software system distributed among the terminals, the software system further comprising,

an access right manager and a filter which evaluates access rights of users to access the access control objects, wherein the access right manager has a data structure in the form of a tree for arranging the access controlled objects and wherein the tree includes a plurality of nodes which each contain a list of permitted

users or user groups respectively, of an access controlled object and for each user or user group respectively, include a list of methods of use.

6. The network of claim 5, wherein the filter is adapted to further evaluate additional data occurring while a user has access to an access control object, monitoring a change in the access rights, and triggering withdrawal of the access rights to the access controlled object.

7. A network, comprising:

a plurality of terminals connected by a bus;

a plurality of access control objects; and

a software system adapted to reserve use of a first one the access control objects by a user via one of the terminals, wherein the software system further comprises a filter adapted to continuously monitor dynamic data affecting access rights to the first control object and, in response to the dynamic data, to generate a message indicating withdrawal of the access rights of the user to the first access control object, the software system being adapted to release the reservation of the first access control object in response to the message from the filter.